



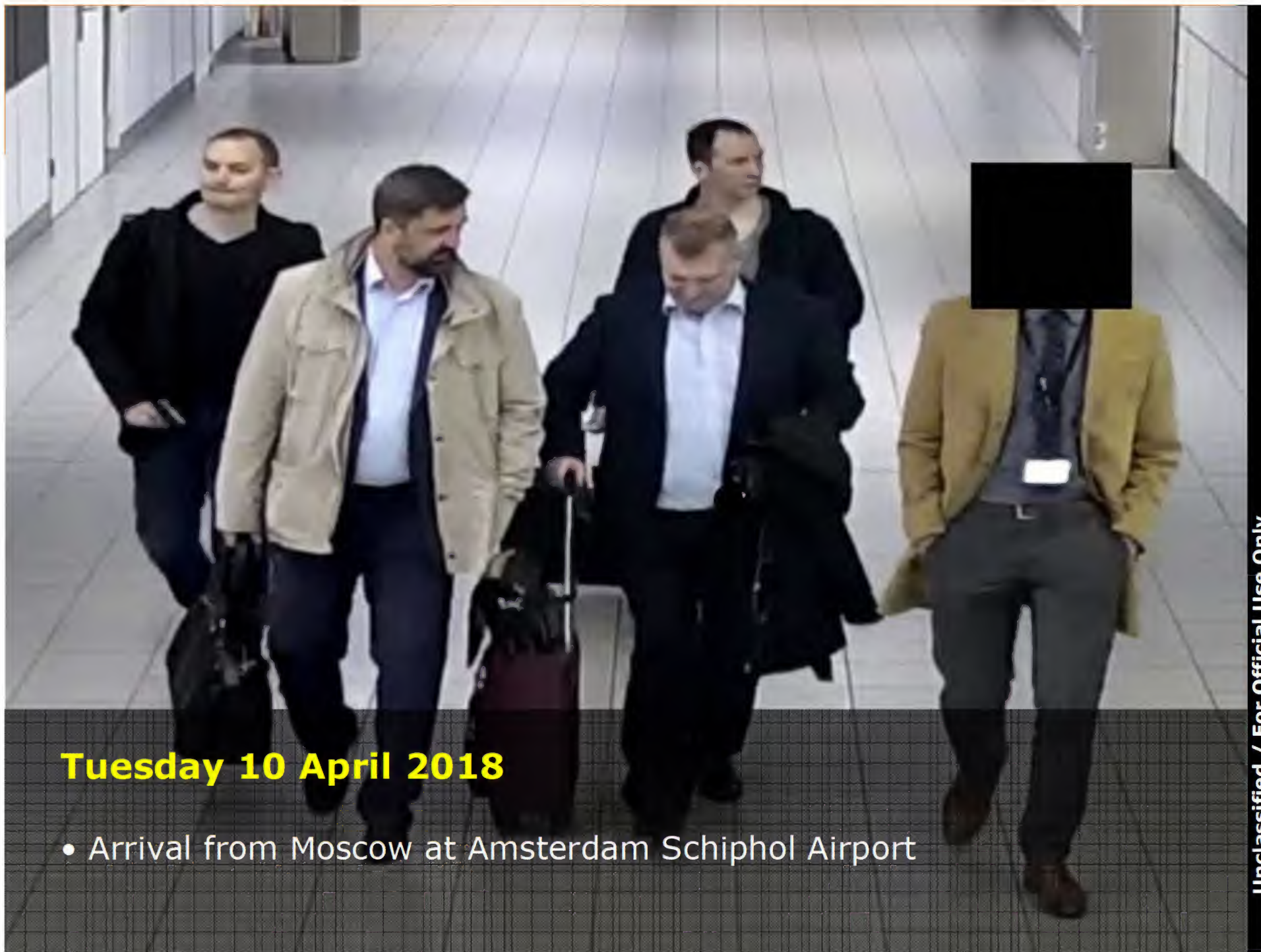
Ministry of Defence

GRU close access cyber operation against OPCW

Genmaj. O. Eichelsheim

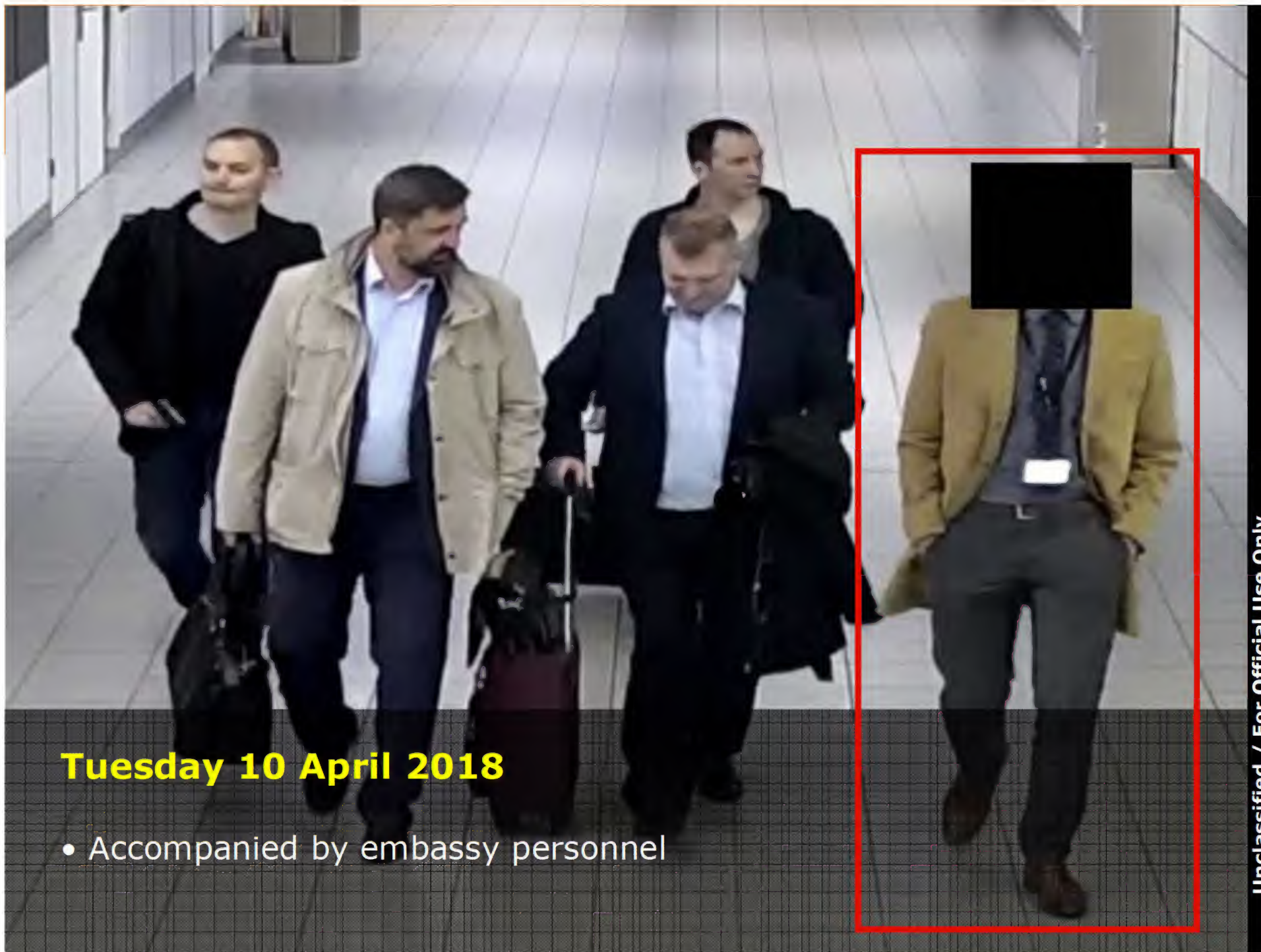
Defence Intelligence &
Security Service

4 October 2018



Tuesday 10 April 2018

- Arrival from Moscow at Amsterdam Schiphol Airport



Tuesday 10 April 2018

- Accompanied by embassy personnel



Overview of Russian persons

- Diplomatic passports

Aleksei MORENETS



Name: Aleksei Sergeyvich MORENETS

Date of birth: 31-07-1977

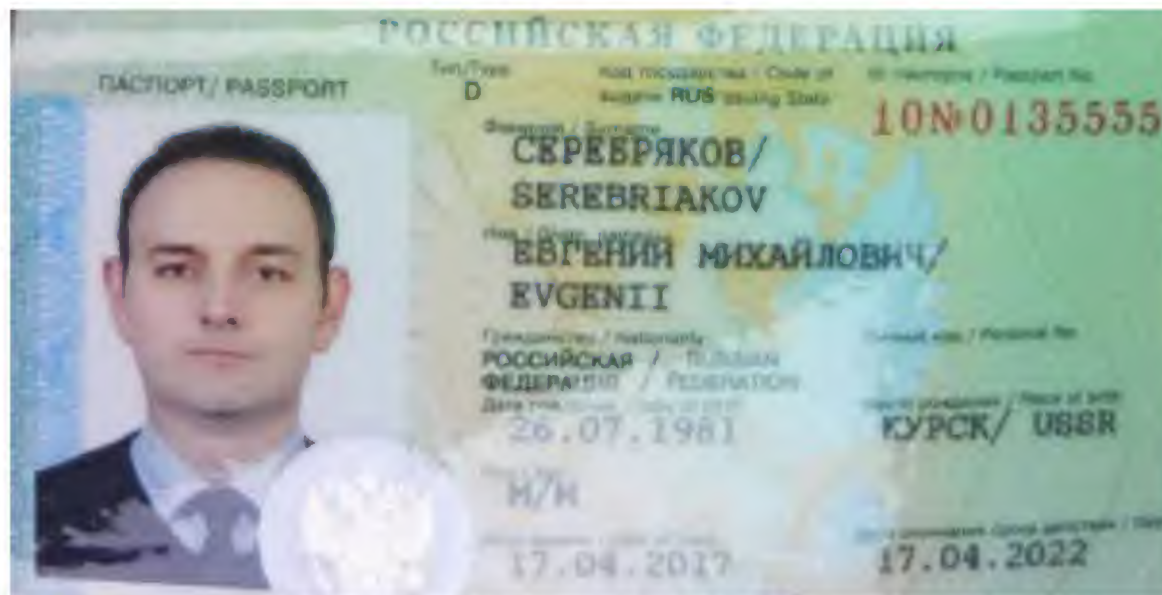
Place of birth: Moermanskaya Oblast

Passport nr: 100135556

Role: Cyber operator



Evgenii SEREBRIAKOV



Name: Evgenii Mikhaylovich SEREBRIAKOV
(a.k.a. SEREBRYAKOV)

Date of birth: 26-07-1981

Place of birth: Kursk

Passport nr: 100135555

Role: cyber operator



Oleg SOTNIKOV



Name: Oleg Mikhaylovich SOTNIKOV

Date of birth: 24-08-1972

Place of birth: Ulyanovsk

Passport nr: 120018866

Role: HUMINT support



Alexey MININ



Name: Alexey Valeryevich MININ

Date of birth: 27-05-1972

Place of birth: Perm Oblast

Passport nr: 120017582


Role: HUMINT support

Unclassified / For Official Use Only

Bestuurder 2 Minin, 27-05-1972

[illegible]

Mourner	: Aleksey Minin
Address	: Pickersley str 8
Phone	: 1735 HOBROW
	Russia
Host address	: Aleksey Minin
Destination	:

Hourly rate : CITROEN C3 (HD)
Kendaraan : PF-934-R (NX-508-T)
Subsidiary : 

RENTAL - PRESENT

NAME: [Redacted]
ADDRESS: [Redacted]
CITY: [Redacted]
STATE: [Redacted]
ZIP: [Redacted]

DATE OF BIRTH: [Redacted]
SEX: [Redacted]
DRIVER'S LICENSE: [Redacted]
EXPIRATION DATE: [Redacted]

VEHICLE TYPE: [Redacted]
MAKE: [Redacted]
MODEL: [Redacted]
YEAR: [Redacted]
VIN: [Redacted]

INSURANCE: [Redacted]
COVERAGE: [Redacted]
AGENT: [Redacted]

REMARKS: [Redacted]

DATE OF RENTAL: [Redacted]
TIME OF RENTAL: [Redacted]
LOCATION: [Redacted]

ACCESSOIRES

check-out	check-in
<input type="checkbox"/> airconditioning	<input type="checkbox"/>
<input type="checkbox"/> autoradio	<input type="checkbox"/>
<input type="checkbox"/> radio / CD fronte	<input type="checkbox"/>
<input type="checkbox"/> navigatie CD / DVD	<input type="checkbox"/>
<input type="checkbox"/> handremmen	<input type="checkbox"/>
<input type="checkbox"/> antenne	<input type="checkbox"/>
<input type="checkbox"/> leik / gereedschapen	<input type="checkbox"/>
<input type="checkbox"/> wielkappen/wegens	<input type="checkbox"/>
<input type="checkbox"/> rijschoolcard	<input type="checkbox"/>
<input type="checkbox"/> zonn/winterbanden	<input type="checkbox"/>
<input type="checkbox"/> aantal stalen	<input type="checkbox"/>
<input type="checkbox"/> overige:	<input type="checkbox"/>

DAMAGE:
YES / NO

☐ Het voertuig is zonder schade uitgegeven

INNAME / CHECK-IN

Kleur: [Redacted] Oor: [Redacted] Haar: [Redacted]

FRONT

BACK

RIGHT

LEFT

DATE & TIME

☐ Het voertuig is zonder schade ingekomen

Huurder verklaart akkoord te gaan met de hieronder genoemde algemene voorwaarden van de BOVAG Verhuurbedrijven. Huurder verklaart akkoord te gaan met de volgende voorwaarde op de overeenkomst en een exemplaar van deze overeenkomst wordt het voertuig zodanig afgegeven en beschreven te hebben ontvangen. Verhuurder verklaart dat het voertuig op het moment van de aanvang van de huurperiode in goede staat verkeert. Zowel huurder als de in de overeenkomst genoemde bestuurder(s) zijn hoofdelijk aansprakelijk voor nakoming van alle verplichtingen die uit deze overeenkomst voortvloeien.

Indien u niet in de gelegenheid bent geweest dit formulier te ondertekenen of heeft een opmerking over de staat van het voertuig, dan dient u dit binnen 2 uur na ontvangst van het voertuig te melden aan onze vestiging.

CHECK OUT

Handtekening en naam huurtar/bestuuder _____

CHECK IN

Handtekening en naam huurtar/bestuuder _____

Handtekening en naam verhuurder _____

Handtekening en naam verhuurder _____

BOVAG



Reconnaissance of OPCW and surroundings

- Photos taken on 11 April, found on MININ's camera



Reconnaissance of OPCW and surroundings

- Photo taken on 12 April, found on MININ's camera



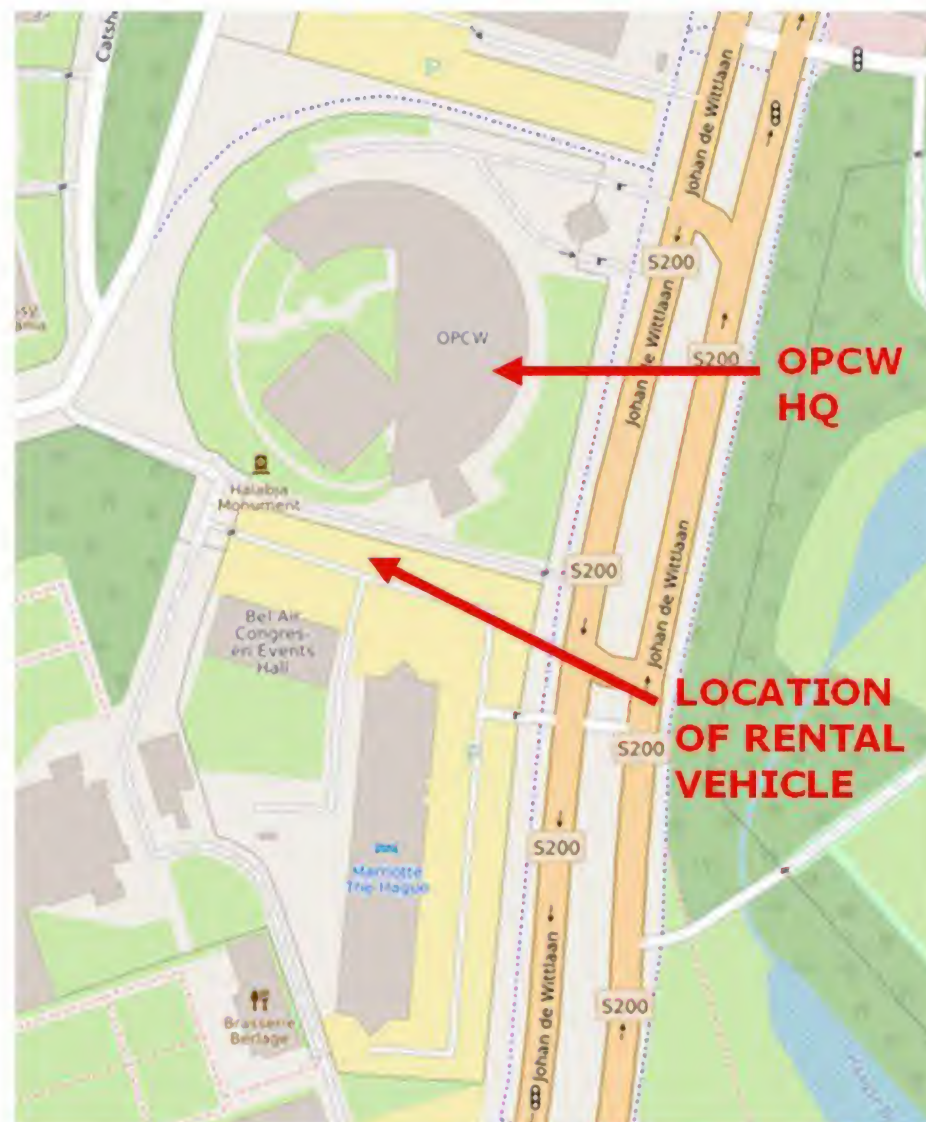
Reconnaissance of OPCW and surroundings

- Photo taken on 13 April, found on MININ's camera



Situation map

- Location of rental vehicle on Friday 13 April





Connected to:

-Smartphone
(4G)

-WiFi panel
antenna

Computer

WiFi panel
antenna
(covered)

Bag with
battery

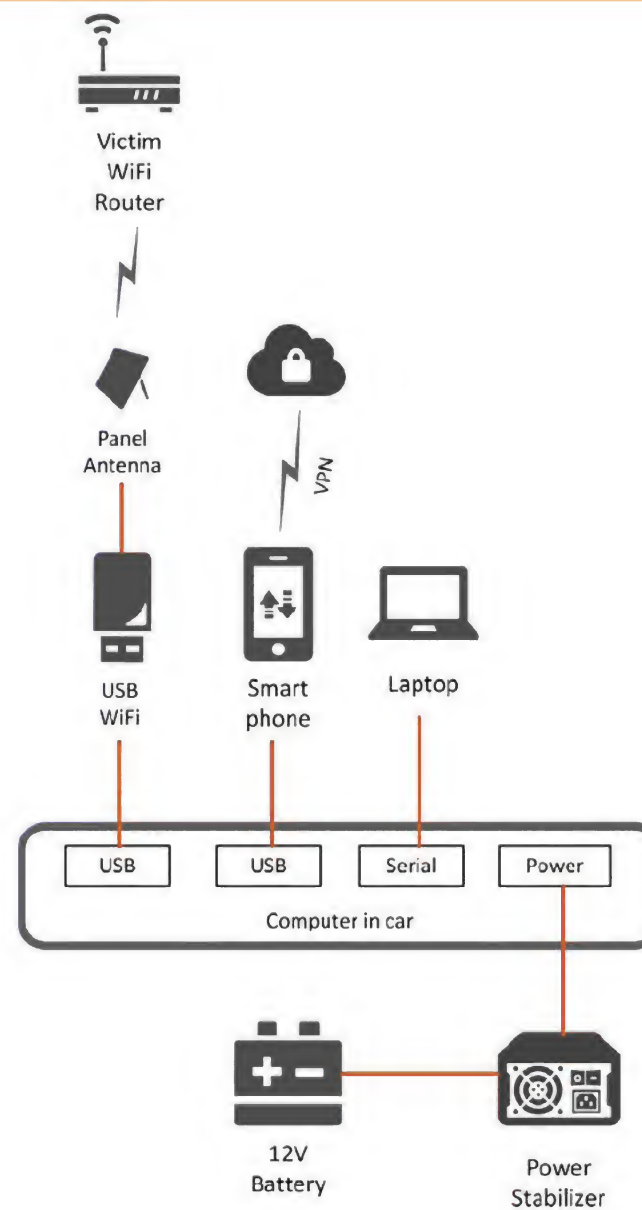
Transformer

Specialist equipment in vehicle

- Setup for hacking WiFi connections



Schematische weergave





WiFi panel antenna

- Hidden under coat





Battery

- Power supply for equipment
- Purchased in The Hague



SPORT BV

20-18-2018 15:14
KEE 000034
VERBODEN 4219.85
EXL BTW 2 4381.53
BTW 2 4381.12
CONTANT € 219.65

TEN, MOTOREN & WATERSPORTARTIKELN

KONTANTBON 624399 Datum: 10/04/18 Pagina 1

Artikel	Omschrijving	Aantal	Prjs	Kort.	Bedrag
GR008100	53 Ah onderhoudsvrij	1.00	100.65		100.65
00449007	MinnKota MK-110PE Acculader po	1.00	119.00		119.00

Exclusief BTW 181,53 BTW hoog 38,12 BTW laag TOTAAL INCL. € 219,65







Operational modus operandi

- Security awareness
- Tried to destroy smartphone during disruption operation



Operational modus operandi

- Security awareness
- GRU intelligence officers took their trash out of their hotel rooms



Operational modus operandi

- Cash money: 20.000 Euro's and 20.000 dollars

OPCW	09-04-2018 07:09:46
https://www.google.ru/maps/search/OPCW/@42.7111121,3.5078125,3z	09-04-2018 07:09:46
Organization for the Prohibition Chemical Weapos	09-04-2018 07:10:16
Organization for the Prohibition Chemical Weapos	09-04-2018 07:10:16
https://www.google.ru/maps/search/Organization+for+the+Prohibition+Chemical+Weapos/@42.7111121,3.5078125,3z	09-04-2018 07:10:16
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:17
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:17
https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.09096,4.2810983,17z/data=!3m1!4b1!4m5!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287	09-04-2018 07:10:17
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:27
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:27
https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.090136,4.281903,17z/data=!4m5!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287	09-04-2018 07:10:27
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:32
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:32
https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.0900569,4.2822248,17z/data=!4m5!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287	09-04-2018 07:10:32
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
https://www.google.ru/maps/place/The+Hague+Marriott+Hotel/@52.0900569,4.2822248,17z/data=!4m12!1m6!3m5!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!2sOrganisation+for+the+Prohibition+of+Chemical+Weapons!8m2!3d52.09096!4d4.283287!3m4!1s0x0:0xc44f7f20fe9c5077!8m2!3d52.0900298!4d4.2824558	09-04-2018 07:10:39

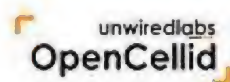
Online searches from SEREBRIAKOV's laptop

- Indicating interest in OPCW headquarters building and immediate surroundings



Additional specialist equipment

- Carried by SEREBRIAKOV
- Intended for hacking WiFi networks



DATA STATS DOCS ENTERPRISE COMMUNITY SIGN IN

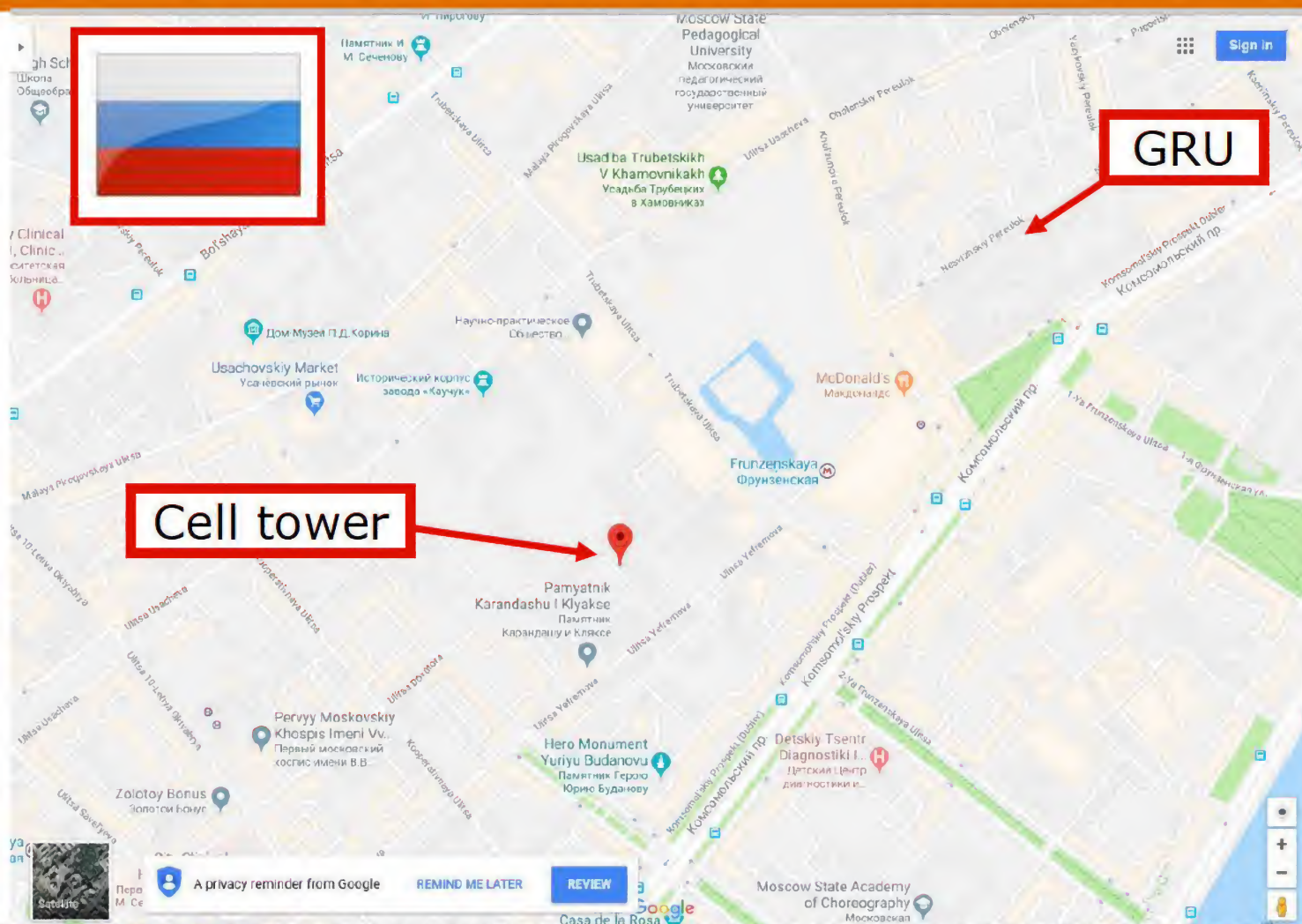
The world's largest Open Database of Cell Towers

Locate devices without GPS, explore Mobile Operator coverage and more!



Sony Xperia F3311

- Activated on 9 April, through cell tower in Moscow (GSM MCC: 250 MNC: 20 LAC: 27813 CID: 197679381)



CID: 197679381

- Nearest cell tower to known GRU barracks at Komsomolsky Prospekt 20, Moscow



ИП Шагинян Бениамин Нариманович
Адрес регистрации: 125252, г. Москва,
ул. 2-я Песчаная, д. 3, кв. 128 8-495-205-ЕЗ-39
ИНН 4029008858
ОГРНИП 313774628000948

Квитанция ГР № 001832

Дата выдачи "10" апреля 2018 г.

Откуда / Starting point
Несви́зхский переулoк

Куда / Point of destination
Аэропорт Шереметьево
терм. F

Показания таксометра

Пробег	32 км	Простой	—
Итого	842,00 руб. <i>восемьсот сорок два рубля 00 коп.</i> (сумма прописью)		

Водитель *Сидоров С.В.* подпись

Заказчик *Моренко* подпись

М.П.

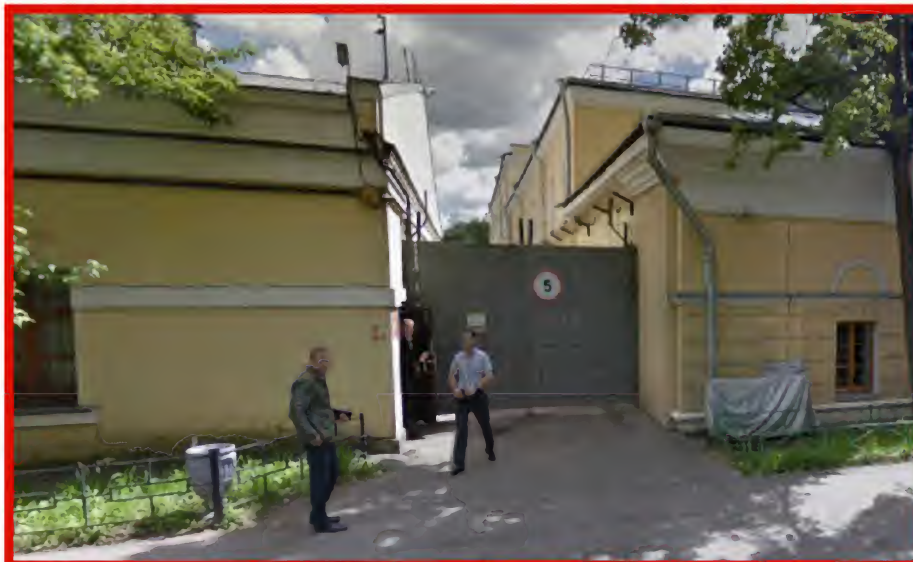
Отпечатано ООО "01-Принт" www.print.ru Тел.: 737-72-60
115191, г. Москва, ул. Большая Тульская, д. 10, стр. 5 ИФН 772507048
Зат № 11/04/2018 Терез 1800 штуч

Nesvizhskiy Pereulok

GRU

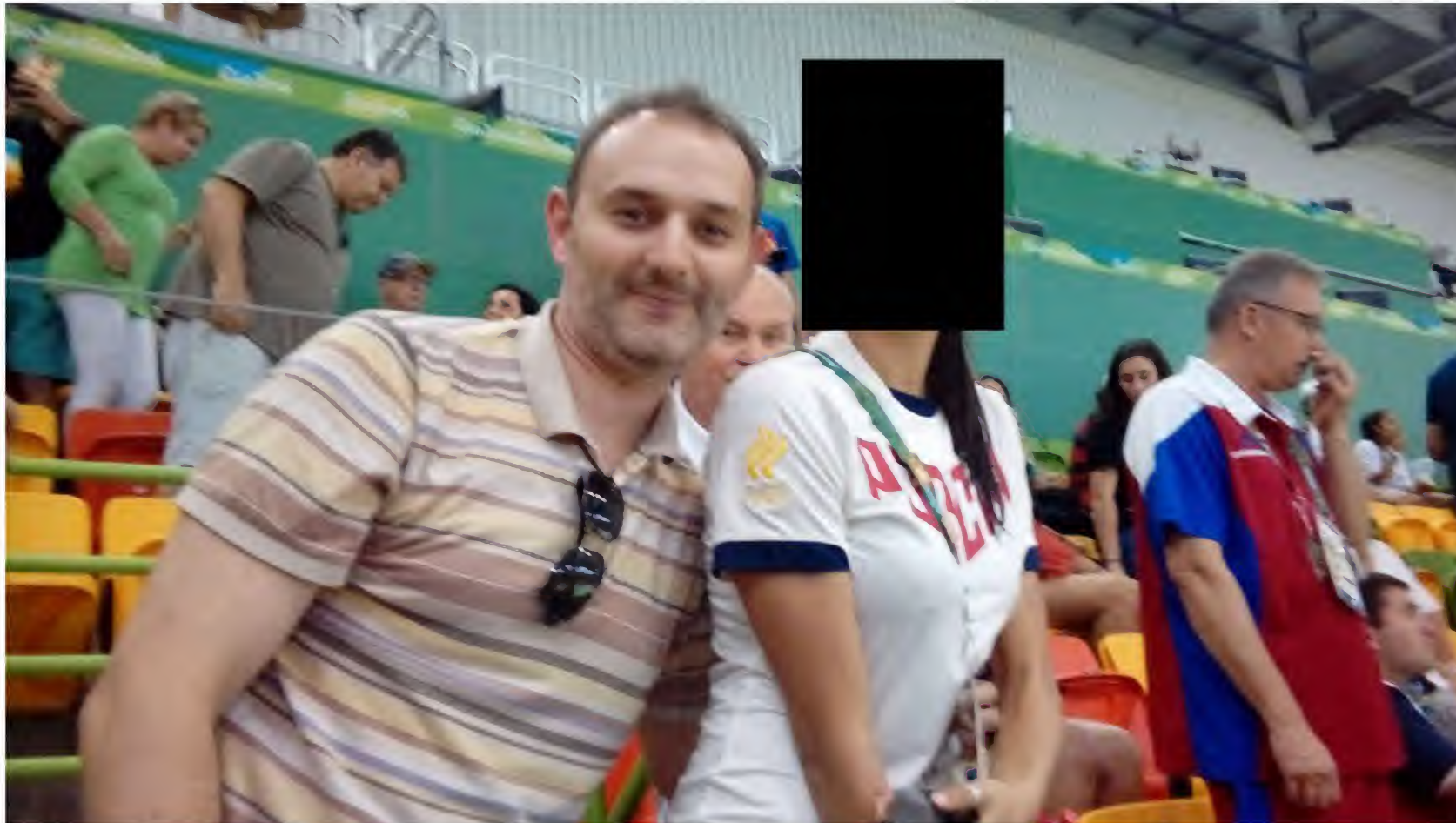
MORENETS' taxi receipt

- From Nesvizhskiy Pereulok to Moscow Sheremetyevo airport
- Date: 10 April 2018



Rear entrance of GRU barracks

- Opening onto Nesvizhskiy Pereulok



Previous operations: photo on SEREBRIAKOV's laptop

- 14 August 2016: Olympic Games in Brazil (picture above taken on 16.39, 14-08-2016 with LG-K350ds)



Network Name	Name Type	First Connect	Last Connected	Managed	DNS Suffix	Gateway Mac Address	Profile GUID	Location (LAT/LON)
Sheremetyevo Wi-Fi	Wireless	2016-09-17 19:10:57 +00:00	2016-09-17 19:10:57 +00:00	Unchecked	<о т с у т с т в у е т>	B4-E9-B0-C9-1E-40	{7D30FD49-1E32-4618-8278-AFF127C2F288}	Airport, Khimki, Russia
LP_Public	Wireless	2016-09-20 20:17:39 +00:00	2016-09-20 20:29:12 +00:00	Unchecked	lausanne-palace.net	00-90-0B-29-02-D7	{FC1F8A2C-7959-4C0A-AE0D-6ACAA049420}	Lausanne, Switzerland
Hotel Alpha-Palmiers	Wireless	2016-09-20 21:26:51 +00:00	2016-09-22 08:59:34 +00:00	Unchecked	monzoon.net	00-1A-A2-9F-9C-AE	{7E6EC1D0-6B1A-467E-A81D-DFFFFF2375E69}	Lausanne, Switzerland
GMKLhotel	Wireless	2017-12-16 03:21:01 +00:00	2017-12-22 12:39:21 +00:00	Unchecked	localdomain	90-E2-BA-58-ED-FB	{64746B9B-1E16-4366-AE08-38596037B691}	Kuala Lumpur, Malaysia
Palace-Hotel-Guests	Wireless	2018-04-10 22:58:44 +00:00	2018-04-12 09:53:14 +00:00	Unchecked	hotspot.internet-for-guests.com	D0-BF-9C-3A-66-B5	{2B8E00FF-9942-4818-A5B9-B0FC6DB523D2}	Noordwijk, Netherlands
Marriott_GUEST	Wireless	2018-04-12 19:08:00 +00:00	2018-04-13 14:12:52 +00:00	Unchecked	<о т с у т с т в у е т>	50-9A-4C-6A-F0-E5	{01E8FAC9-4419-4B38-80B9-9A9F896A5415}	The Hague, Netherlands

Previous operations: WiFi connections made by SEREBRIAKOV's laptop

- Grand Millenium Hotel (Kuala Lumpur, Malaysia) from 16 to 22 December 2017;
- Alpha Palmiers Hotel (Lausanne, Switzerland) from 20 to 22 September 2016;
- Palace Hotel (Lausanne, Switzerland) on 20 September 2016.

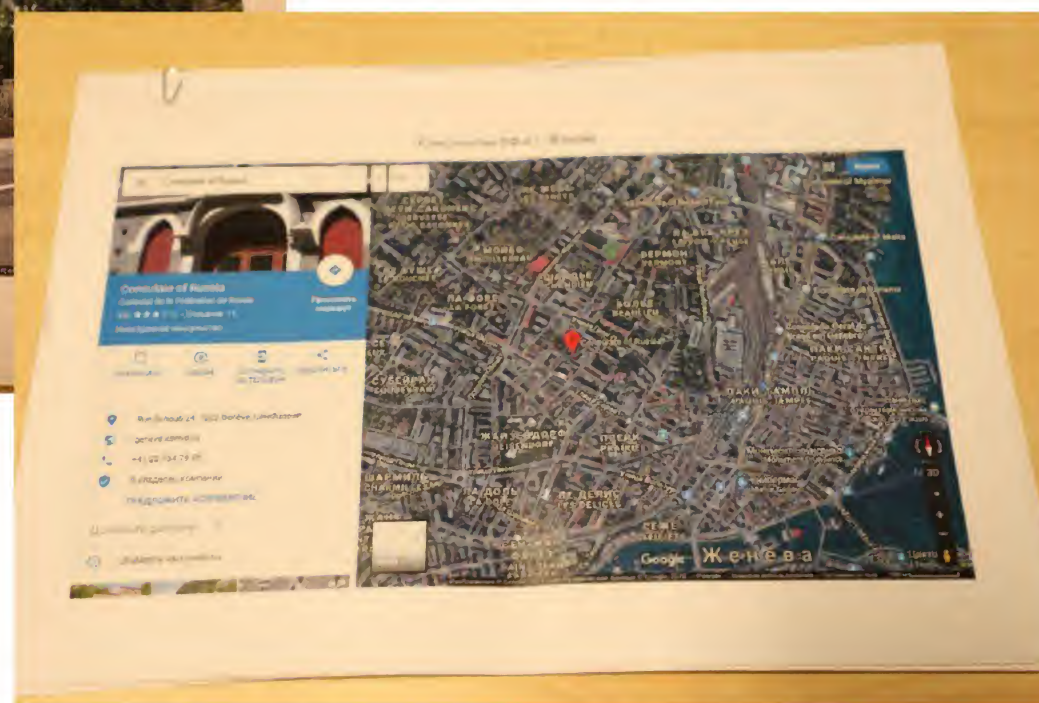


Opera web visits.csv:3274,https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKewTr7eaA0azaAhwTY
Opera web visits.csv:3275,https://www.opcw.org/ru/ 09-04-2018 07:09:33,???????????? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
Opera web visits.csv:3561,https://www.opcw.org/ru/ 09-04-2018 08:05:22,???????????? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
Opera web visits.csv:3936,https://www.opcw.org/ru/admin/OPCW/Fact_Sheets/Russian/Fact_Sheet_3_-_OPCW_Structure.pdf
Opera web visits.csv:2999,https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKewio7-7wxazaAhvSE
Opera web visits.csv:3000,https://www.labor-spiez.ch/ 09-04-2018 06:17:17,LABOR SPIEZ - SPIEZ LABORATORY,0,LINK,, "d
Opera web visits.csv:3001,https://www.labor-spiez.ch/enindex.htm,09-04-2018 06:18:16,LABOR SPIEZ - SPIEZ LABORATORY
Opera web visits.csv:3012,https://www.labor-spiez.ch/enindex.htm,09-04-2018 06:20:00,LABOR SPIEZ - SPIEZ LABORATORY
Opera web visits.csv:3028,http://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3029,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3271,http://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3272,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapon
Opera web visits.csv:3931,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3932,https://www.labor-spiez.ch/enindex.htm,09-04-2018 12:14:28,LABOR SPIEZ - SPIEZ LABORATORY

Austrasse, 3700 Spiez, Швейцария	09-04-2018 07:03:01
https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.05z/data=!4m5!3m4!1s0x478fadb1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0	09-04-2018 07:03:01
https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.03z/data=!4m5!3m4!1s0x478fadb1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0	09-04-2018 07:03:01
https://www.google.ru/maps/@46.6931311,7.6467636,19.03z?dcr=0	09-04-2018 07:03:07
hotels	09-04-2018 07:03:14
https://www.google.ru/maps/search/hotels/@46.6931311,7.6467636,19.03z?dcr=0	09-04-2018 07:03:14

Target: Spiez Laboratory

- Train tickets to Bern
- Online searches for Spiez laboratory
- Google-maps print-outs of Russian diplomatic facilities in Bern



Google Maps print-outs

- Russian diplomatic facilities in Bern and Geneva



DNR: FCTDHXS ID:0

RESERVERING
RESERVATION
InterCityExpress

CIV 1184

RESERVOIR

→ AANKOMST

17/04 07:38

UTRECHT CENTRAAL → BASEL SBB

17/04 14:47

KLASSE 1

TREIN 255 ICE RIJTOEG 39 ZITPLAATS

NIET ROKEN MET MIDDENGANG 02GANG 02RAAM

04 RESERVERING ALLEEN ICM EEN GELDIG VERVOERERBILLET

849830087650 IR DNR:FCTDHXS Ref:

Den Haag 130418 11:37 CACASH 1/1

PRJIS: EUR *****0.00

Sotnikov, O
04PERSONEN

Passagierslijst:

Naam	Voornaam
Sotnikov	O
Minin	A
Serebriakov	E
Morenets	A

Train tickets to Switzerland

- Departure from Utrecht for Bern via Basel
- Planned date: 17 April 2018